(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－165248
（P2000－165248A）
(43)公開日　平成12年６月16日(2000.6.16)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０３Ｍ　7/00		Ｈ０３Ｍ　7/00		５Ｃ０６３
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00		５Ｃ０７６
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ　1/387		５Ｊ０６４
7/08		7/08	Ｚ	５Ｊ１０４
7/081				９Ａ００１

審査請求　未請求　請求項の数36　ＯＬ　（全 15 頁）

(21)出願番号　特願平10－337258

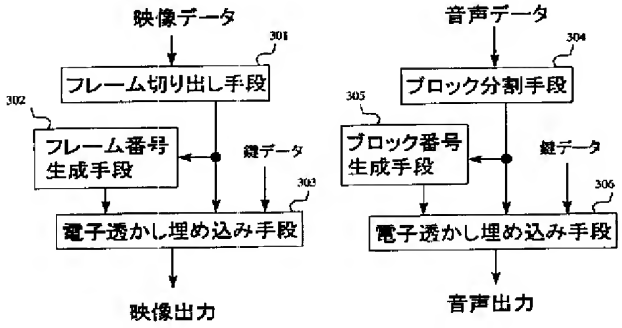
(22)出願日　平成10年11月27日(1998.11.27)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　吉田　淳
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100090273
弁理士　國分　孝悦

最終頁に続く

(54)【発明の名称】　電子透かし埋め込み装置、出力制御装置及びコンピュータ読み取り可能な記憶媒体

(57)【要約】
【課題】　映像と音声を含むコンテンツの著作権を、映像と音声に対して総合的に保護できる電子透かしを上記コンテンツに埋め込む。
【解決手段】　入力された映像データはフレーム切り出し手段３０１によりフレーム分割され、各フレームにフレーム番号が付加される。そして、各フレームとフレーム番号と不揮発性メモリ１０７に記憶されている電子透かし埋め込み位置情報等の鍵データとが電子透かし埋め込み手段３０３に入力され、各フレームにフレーム番号が電子透かしとして埋め込まれる。音声データもブロック分割手段３０４でブロックに分割され、ブロック番号が付加され、各ブロックとブロック番号と鍵データとが電子透かし埋め込み手段３０６に入力され、各ブロックにブロック番号が電子透かしとして埋め込まれる。



1

【特許請求の範囲】

【請求項１】　複数の情報系列を含むコンテンツにおける上記各情報系列に対してそれぞれ埋め込み情報を生成する情報生成手段と、

上記生成された各埋め込み情報を各情報系列に対して電子透かしとして埋め込む埋め込み手段とを設けたことを特徴とする電子透かし埋め込み装置。

【請求項２】　上記情報生成手段が生成する各埋め込み情報が、互いに関連する情報であることを特徴とする請求項１記載の電子透かし埋め込み装置。

【請求項３】　上記情報生成手段が生成する各埋め込み情報が、一致することを特徴とする請求項１記載の電子透かし埋め込み装置。

【請求項４】　上記情報系列を分割して部分情報系列を生成する分割手段を設けると共に、上記情報生成手段は、上記部分情報系列を識別する識別子を生成し、上記埋め込み手段は、上記部分情報系列に上記生成された識別子を電子透かしとして埋め込むことを特徴とする請求項１記載の電子透かし埋め込み装置。

【請求項５】　上記識別子が番号であることを特徴とする請求項４記載の電子透かし埋め込み装置。

【請求項６】　上記各情報系列に埋め込まれる上記埋め込み情報を組み合わせることにより一つの情報を表すことを特徴とする請求項１記載の電子透かし埋め込み装置。

【請求項７】　上記埋め込み情報の少なくとも１つが誤り訂正符号化されていることを特徴とする請求項１記載の電子透かし埋め込み装置。

【請求項８】　上記埋め込み情報を組み合わせることによって表される情報が誤り訂正符号化されていることを特徴とする請求項６記載の電子透かし埋め込み装置。

【請求項９】　上記情報生成手段が、上記情報系列のうちの少なくとも一つから演算によって埋め込み情報を生成し、上記埋め込み手段が、上記埋め込み情報を、上記情報系列のうちの少なくとも他の一つに電子透かしとして埋め込むことを特徴とする請求項１記載の電子透かし埋め込み装置。

【請求項１０】　上記情報生成手段が、上記埋め込み情報として、上記情報系列の全体又は所定の部分の圧縮値を求めることを特徴とする請求項９記載の電子透かし埋め込み装置。

【請求項１１】　上記情報生成手段によって生成された上記埋め込み情報を暗号化する暗号化手段を設けたことを特徴とする請求項９記載の電子透かし埋め込み装置。

【請求項１２】　上記情報生成手段が、上記埋め込み方法として、上記情報系列の全体又は所定の部分のディジタル署名を求めることを特徴とする請求項９記載の電子透かし埋め込み装置。

【請求項１３】　上記情報系列のうち少なくとも二つを分割して部分情報系列を生成する分割手段を設け、上記

2

情報生成手段は、上記情報系列のうちの少なくとも一つより生成された上記部分情報系列を埋め込み情報とし、上記埋め込み手段は、上記埋め込み情報を、上記情報系列のうちの少なくとも他の一つより生成された部分情報系列に電子透かしとして埋め込むことを特徴とする請求項１記載の電子透かし埋め込み装置。

【請求項１４】　上記埋め込み情報である上記部分情報系列を暗号化する暗号化手段を設けたことを特徴とする請求項１３記載の電子透かし埋め込み装置。

【請求項１５】　上記情報系列のうち少なくとも一つを暗号化する暗号化手段を設けると共に、上記情報生成手段は、上記暗号化を復号するための復号鍵を埋め込み情報として生成し、上記埋め込み手段が、上記復号鍵の埋め込み情報を情報系列の少なくとも他の一つに埋め込むことを特徴とする請求項１記載の電子透かし埋め込み装置。

【請求項１６】　上記複数の情報系列が音声情報及び映像情報であることを特徴とする請求項１記載の電子透かし埋め込み装置。

【請求項１７】　上記複数の情報系列が複数のオブジェクトを表すデータを含むコンテンツ中の所定のオブジェクトを表すデータであることを特徴とする請求項１記載の電子透かし埋め込み装置。

【請求項１８】　複数の情報系列を含むコンテンツを出力する出力手段と、

上記コンテンツにおける上記各情報系列を分割して部分情報系列とする分割手段と、

上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する電子透かし抽出手段と、

上記抽出された各埋め込み情報を比較し、比較結果に応じて上記出力手段を制御する比較手段とを設けたことを特徴とする出力制御装置。

【請求項１９】　複数の情報系列を含むコンテンツを出力する出力手段と、

上記コンテンツにおける上記各情報系列を分割して部分情報系列とする分割手段と、

上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する電子透かし抽出手段と、

上記埋め込み情報の一つに対して演算を行う演算手段と、

上記演算手段により求められた値と上記部分情報系列とを比較し、比較結果に応じて上記出力手段を制御する比較手段とを設けたことを特徴とする出力制御装置。

【請求項２０】　上記演算手段は、上記部分情報系列の全体又は一部分の圧縮値を求めることを特徴とする請求項１９記載の出力制御装置。

【請求項２１】　上記電子透かし抽出手段が抽出した上記埋め込み情報に施されている暗号化を復号する復号手段を設けたことを特徴とする請求項１９記載の出力制御装置。

【請求項２２】　上記演算手段によって求められた演算結果を暗号化する暗号化手段を設けたことを特徴とする請求項１９記載の出力制御装置。

【請求項２３】　上記コンテンツに含まれる複数の情報系列が、映像情報及び音声情報であることを特徴とする請求項１８又は１９記載の出力制御装置。

【請求項２４】　上記コンテンツに含まれる情報系列が、複数のオブジェクトを表すデータを含むコンテンツ中の所定のオブジェクトを表すデータであることを特徴とする請求項１８又は１９記載の出力制御装置。

【請求項２５】　複数の情報系列を含むコンテンツにおける上記各情報系列の少なくとも一つの情報系列を分割して部分情報系列とする分割手段と、
上記部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する電子透かし抽出手段と、
上記埋め込み情報を上記コンテンツに含まれる情報系列の一つとして出力する出力手段を設けたことを特徴とする出力制御装置。

【請求項２６】　上記電子透かし抽出手段により抽出された埋め込み情報に施されている暗号の復号を行う復号手段を設けたことを特徴とする請求項２５記載の出力制御装置。

【請求項２７】　上記コンテンツに含まれる複数の情報系列が映像情報及び音声情報であると共に、上記電子透かしが埋め込まれる被埋め込み情報が音声又は映像情報であり、上記埋め込み情報が映像又は音声情報であることを特徴とする請求項２５記載の出力制御装置。

【請求項２８】　上記コンテンツに含まれる情報系列、上記被埋め込み情報及び上記埋め込み情報が、複数のオブジェクトを表すデータを含むコンテンツ中の所定のオブジェクトを表すデータであることを特徴とする請求項２５記載の出力制御装置。

【請求項２９】　少なくとも一つの暗号化された情報系列と少なくとも一つの電子透かしが埋め込まれた情報系列とを含む複数の情報系列を含むコンテンツにおける上記電子透かしが埋め込まれた情報系列から埋め込み情報を抽出する抽出手段と、
上記埋め込み情報を復号鍵として上記情報系列に施された暗号を復号する復号手段を設けたことを特徴とする出力制御装置。

【請求項３０】　上記暗号化された情報系列が映像又は音声情報であり、上記電子透かしが埋め込まれた情報系列が音声又は映像情報であることを特徴とする請求項２９記載の出力制御装置。

【請求項３１】　上記暗号化された情報系列及び上記電子透かしが埋め込まれた情報系列が、複数のオブジェクトを表すデータを含むコンテンツ中の所定のオブジェクトを表すデータであることを特徴とする請求項２９記載の出力制御装置。

【請求項３２】　複数の情報系列を含むコンテンツにおける上記各情報系列に対してそれぞれ埋め込み情報を生成する処理と、
上記生成された各埋め込み情報を各情報系列に対して電子透かしとして埋め込む処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項３３】　複数の情報系列を含むコンテンツを出力する処理と、
上記コンテンツにおける上記各情報系列を分割して部分情報系列とする処理と、
上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する処理と、
上記抽出された各埋め込み情報を比較し、比較結果に応じて上記出力を制御する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項３４】　複数の情報系列を含むコンテンツを出力する処理と、
上記コンテンツにおける上記各情報系列を分割して部分情報系列とする処理と、
上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する処理と、
上記埋め込み情報の一つに対して演算を行う処理と、
上記演算により求められた値と上記部分情報系列とを比較し、比較結果に応じて上記出力を制御する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項３５】　複数の情報系列を含むコンテンツにおける上記各情報系列の少なくとも一つの情報系列を分割して部分情報系列とする処理と、
上記部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する処理と、
上記埋め込み情報を上記コンテンツに含まれる情報系列の一つとして出力する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項３６】　少なくとも一つの暗号化された情報系列と少なくとも一つの電子透かしが埋め込まれた情報系列とを含む複数の情報系列を含むコンテンツにおける上記電子透かしが埋め込まれた情報系列から埋め込み情報を抽出する抽処理と、
上記埋め込み情報を復号鍵として上記情報系列に施された暗号を復号する処理とを実行するためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ビデオ、テレビ番組、映画等の映像及び音声を含むコンテンツに対して著作権保護のための電子透かしを埋め込む場合に用いて好適な電子透かし埋め込み装置、及び記録された上記コンテンツの再生出力等の出力制御に用いて好適な出力制御装置、及びそれらに用いられるコンピュータ読み取り可能な記憶媒体に関するものである。

【０００２】
【従来の技術】従来より、画像、音楽、映画等のコンテンツの不正なコピーを防ぐための手法の一つとして電子透かしと呼ばれる手法がある。電子透かしとは、不正を防止するための情報を、人間に知覚できない形でコンテンツに埋め込む手法である。その場合、ディジタルコンテンツはそのままの状態で情報を埋め込むが、アナログコンチンツはディジタル化した後、情報を埋め込む。
【０００３】以下、コンテンツに対する電子透かしの従来の埋め込み方法の代表的なものについて述べる。静止画像に対する電子透かしの情報埋め込み方式の代表的なものとして、ディジタル画像の場合でいえば、画素の色相、明度等にあたる、ディジタルコンテンツのデータ値に演算を施して電子透かしを埋め込む手法がある。この手法の代表的なものとして、ディジタルコンテンツをブロックに分割し、ブロック毎に＋１と－１の組み合わせである予め決められた透かしパターンを足し込むというＤｉｇｉｍａｒｃ社、米国特許５，６３６，２９２号の手法がある。
【０００４】他の静止画像に対する電子透かし埋め込み方法として、ディジタルコンテンツに対して、高速フーリエ変換、離散コサイン変換、ウェーブレット変換等の周波数変換を行い、周波数領域に透かし情報を加えた後、逆周波数変換を行うことにより埋め込みを行う手法がある。
【０００５】上記高速フーリエ変換による手法では、入力コンテンツは、ＰＮ系列を加えられて拡散された後、ブロックに分割される。そして、ブロック毎にフーリエ変換が施され、１ブロックに１ビットの透かし情報が埋め込まれる。この透かし情報が埋め込まれたブロックは逆フーリエ変換が施され、再び最初と同じＰＮ系列が加えられて電子透かしが埋め込まれたコンテンツが得られる。これは、大西、岡、松井、”ＰＮ系列による画像への透かし署名法”１９９７年、暗号と情報セキュリティシンポジウム講演論文集、ＳＣＩＳ９７－２６Ｂに詳しい。
【０００６】離散コサイン変換による手法は、ブロックに分割し、ブロック毎に離散コサイン変換をする。そして、１ブロックに１ビットの情報を埋め込んだ後、逆変換をして電子透かし埋め込み済みコンテンツを生成する。これは、中村、小川、高嶋”ディジタル画像の著作権保護のための周波数領域における電子透かし方式”１９９７年、暗号と情報セキュリティシンポジウム講演論文集、ＳＣＩＳ９７・２６Ａに詳しい。
【０００７】ウェーブレット変換による手法は、入力コンテンツをブロック分割する必要のない手法である。これは、石塚、酒井、櫻井、”ウェーブレット変換を用いた電子すかし技術の安全性と信頼性に関する実験的考察”１９９７年、暗号と情報セキュリティシンポジウム講演論文集、ＳＣＩＳ９７－２６Ｄに詳しい。
【０００８】音声データの場合も、静止画像と同様に、ブロック化した後に周波数変換、電子透かしの埋め込み、逆周波数変換を行う方法により、電子透かしの埋め込みが可能である。具体的には、周期の異なる三角関数を基底関数群として、それらの１次結合の形で表される１次元音声データの基底関数群から幾つかの基底関数を取り出し、位相をいくらかずらした後、再び音声データに復元しても、元のデータとの違いを知覚することができないという人間の聴覚特性を利用した方法がある。
【０００９】また、１次元実数値関数として表されるディジタル音声データをウェーブレット変換して、得られたウェーブレット係数に対し埋め込みを行うという方法がある。この方法は、静かな音は、大きな音にかき消されてしまうという聴覚特性を利用したものである。これらの手法の詳細については、井上杉「電子透かし―マルチメディア自体の暗号システム」丸山学芸図書に詳しい。
【００１０】また、電子透かしの静止画像への埋め込み、音声への埋め込みの他、動画像データへの電子透かし埋め込み技術として、動きベクトルに埋め込む方法や、２台の微妙に異なる角度から被写体を撮影するカメラからの動画像を組み合わせる方法が知られている。
【００１１】次に、一般的なフレーム内符号化手段とフレーム間符号化手段を備えた動画像圧縮方式ＭＰＥＧの原理について説明した後、電子透かしを動画像データの動きベクトルに埋め込む手法について説明する。ＭＰＥＧでは、フレーム間の差分を取ることで時間軸方向の冗長度を落とし、これによって得られた差分データをＤＣＴ及び可変長符号化処理して空間方向の冗長度を落とすことによって全体として高能率符号化を実現する。上記時間軸方向の冗長度については、動画の場合には連続したフレームの相関が高いことに着目し、符号化しようとするフレームと時間的に先行又は後行するフレームとの差分をとることによって冗長度を落とすことが可能となる。
【００１２】そこで、フレーム内で符号化する符合化モードで得られるインドラ符号化画像（Ｉ－ピクチャ）の他に、時間的に先行するフレームとの差分値を符号化する前方予測符号化画像（Ｐ－ピクチャ）と、時間的に先行するフレーム又は後行するフレームとの差分値、或いはそれらの両フレームからの補間フレームとの差分値の内最もデータ量が少ないものを符号化する両方向予測符号化画像（Ｂ－ピクチャ）とを有し、これらの符合化モードによる各フレームを所定の順序で組み合わせている。
【００１３】ＭＰＥＧにおいては、上述のＩ－ピクチャ、Ｐ－ピクチャ、Ｂ－ピクチャをそれぞれ１枚、４枚、１０枚で１単位（ＧＯＰ）とし、先頭にＩ－ピクチャを配し、２枚のＢ－ピクチャとＰ－ピクチャとを繰り返し配する組み合わせを推奨しており、一定周期でＩ－

ピクチャを置くことによって、逆再生等の特殊再生やこのＧＯＰを単位とした部分再生を可能とするとともにエラー伝播の防止を図っている。

【００１４】また、フレーム中で新たな物体が現れた場合には、時間的に先行するフレームとの差分を取るよりも、後行するフレームとの差分を取った方がその差分値が少なくなる場合がある。そこで、ＭＰＥＧでは、上述のような両方向予測符号化を行い、より高能率な圧縮を行っている。

【００１５】また、ＭＰＥＧでは動き補償を行う。即ち、８画素×８画素のブロックを輝度データについて４ブロック、色差データについて２ブロック集めた所定ブロック（マクロブロック）単位で、先行又は後行フレームの対応ブロック近傍のマクロブロックとの差分をとり、一番差が少ないマクロブロックを探索することによって動きベクトルを検出し、この動きベクトルをデータとして符号化する。

【００１６】復号の際には、この動きベクトルを用いて先行又は後行フレームの対応マクロブロックデータを抽出し、これによって動き補償を用いて符号化された符号化データの復号を行う。上述のような動き補償に際しては、時間的に先行するフレームを一旦符号化した後、再度復号したフレームを得て先行フレームとし、このフレームにおけるマクロブロックと符号化しようとするフレームのマクロブロックとを用いて動き補償が行われる。

【００１７】そこで、電子透かしを動きベクトルに埋め込む方式では、一つの動きベクトルの移動を透かし情報のビット列の１ビットに対応させる。即ち、このビットの値を１にしたい場合は、このベクトルを目視では認識不可能な程度移動させ、値を０にしたい場合には、ベクトルを移動させない。この処理を多くの動きベクトルに施すことにより、全ての透かし情報を埋め込む方法を取っている。

【００１８】また、現在標準化作業中のＭＰＥＧ－４においては、複数ビデオプレーンを重ね合せる処理が導入された。これによりマクロブロックごとの符号化に代わり、画像上のオブジェクト単位での符号化など、任意の輪郭の領域での処理が可能となった。輪郭符号化にはＭＭＲや算術符号化が使われる。

【００１９】次に、２台の微妙に異なる角度より被写体を撮影するカメラからの動画像を組み合わせる方法について説明する。一つの被写体に対して微妙に異なる角度から撮影できるように２台のカメラを設置する。被写体を頂点として２台のカメラがなす角度は、非常に小さいので、２台のカメラで撮影した画像は、人間の目では識別できない。

【００２０】２台のカメラをＡ，Ｂとする。カメラＡ，Ｂにより撮影した画像を各々フレーム毎に分割し、それらを（ａ１，ａ２・・・ａｎ）、（ｂ１，ｂ２・・・ｂｎ）とする。カメラＡ，Ｂが撮影した画像のフレームよりランダムに画像を選択し、原画像を作成する。例えば、原画像は（ａ１，ａ２，ｂ３，ａ４，ｂ５・・・ｂｎ）となる。ここで、１フレームを透かし情報のビット列の１ビットに対応させる。即ち、このビットの値を１としたい場合は、フレームを他方のフレームで置き換える。ビツトの値を０としたい場合は、フレームの置き換えを行わない。この処理を多くのフレームに施すことにより、全ての透かし情報を埋め込む。

【００２１】

【発明が解決しようとする課題】従来の、映画等の映像と音声を有するコンテンツに対する電子透かし埋め込み方式は、映像及び音声に対してそれぞれ別個に埋め込みを行うものであった。このため、映像、音声各々単体での著作権は保護することが可能であったが、映像と音声の両方を有するコンテンツとして総合的に著作権を保護するには限界があった。

【００２２】本発明は、上記の問題を解決するために成されたもので、映像及び音声のコンテンツの著作権を総合的に保護できる電子透かしを埋め込むことができるようにすることを目的としている。

【００２３】

【課題を解決するための手段】上記の目的を達成するために、本発明による電子透かし埋め込み装置においては、複数の情報系列を含むコンテンツにおける上記各情報系列に対してそれぞれ埋め込み情報を生成する情報生成手段と、上記生成された各埋め込み情報を各情報系列に対して電子透かしとして埋め込む埋め込み手段とを設けている。

【００２４】また、本発明による出力制御装置においては、複数の情報系列を含むコンテンツを出力する出力手段と、上記コンテンツにおける上記各情報系列を分割して部分情報系列とする分割手段と、上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する電子透かし抽出手段と、上記抽出された各埋め込み情報を比較し、比較結果に応じて上記出力手段を制御する比較手段とを設けている。

【００２５】また、本発明による他の出力制御装置においては、複数の情報系列を含むコンテンツを出力する出力手段と、上記コンテンツにおける上記各情報系列を分割して部分情報系列とする分割手段と、上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する電子透かし抽出手段と、上記埋め込み情報の一つに対して演算を行う演算手段と、上記演算手段により求められた値と上記部分情報系列とを比較し、比較結果に応じて上記出力手段を制御する比較手段とを設けている。

【００２６】また、本発明による他の出力制御装置においては、複数の情報系列を含むコンテンツにおける上記各情報系列の少なくとも一つの情報系列を分割して部分情報系列とする分割手段と、上記部分情報系列に電子透

かしとして埋め込まれている埋め込み情報を抽出する電子透かし抽出手段と、上記埋め込み情報を上記コンテンツに含まれる情報系列の一つとして出力する出力手段を設けている。

【００２７】また、本発明による他の出力制御装置においては、少なくとも一つの暗号化された情報系列と少なくとも一つの電子透かしが埋め込まれた情報系列とを含む複数の情報系列を含むコンテンツにおける上記電子透かしが埋め込まれた情報系列から埋め込み情報を抽出する抽出手段と、上記埋め込み情報を復号鍵として上記情報系列に施された暗号を復号する復号手段を設けている。

【００２８】また、本発明による記憶媒体においては、複数の情報系列を含むコンテンツにおける上記各情報系列に対してそれぞれ埋め込み情報を生成する処理と、上記生成された各埋め込み情報を各情報系列に対して電子透かしとして埋め込む処理とを実行するためのプログラムを記憶している。

【００２９】また、本発明による他の記憶媒体においては、複数の情報系列を含むコンテンツを出力する処理と、上記コンテンツにおける上記各情報系列を分割して部分情報系列とする処理と、上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する処理と、上記抽出された各埋め込み情報を比較し、比較結果に応じて上記出力を制御する処理とを実行するためのプログラムを記憶している。

【００３０】また、本発明による他の記憶媒体においては、複数の情報系列を含むコンテンツを出力する処理と、上記コンテンツにおける上記各情報系列を分割して部分情報系列とする処理と、上記各部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する処理と、上記埋め込み情報の一つに対して演算を行う処理と、上記演算により求められた値と上記部分情報系列とを比較し、比較結果に応じて上記出力を制御する処理とを実行するためのプログラムを記憶している。

【００３１】また、本発明による他の記憶媒体においては、複数の情報系列を含むコンテンツにおける上記各情報系列の少なくとも一つの情報系列を分割して部分情報系列とする処理と、上記部分情報系列に電子透かしとして埋め込まれている埋め込み情報を抽出する処理と、上記埋め込み情報を上記コンテンツに含まれる情報系列の一つとして出力する処理とを実行するためのプログラムを記憶している。

【００３２】また、本発明による他の記憶媒体においては、少なくとも一つの暗号化された情報系列と少なくとも一つの電子透かしが埋め込まれた情報系列とを含む複数の情報系列を含むコンテンツにおける上記電子透かしが埋め込まれた情報系列から埋め込み情報を抽出する抽処理と、上記埋め込み情報を復号鍵として上記情報系列に施された暗号を復号する処理とを実行するためのプログラムを記憶している。

【００３３】

【発明の実施の形態】以下、本発明の実施の形態を図面と共に説明する。図１は、本発明による電子透かし埋め込み装置の実施の形態を示すブロック図である。本装置は、例えば、再生側と録画側の２台のビデオテープレコーダに接続されて用いられる。再生側ビデオテープレコーダでは、電子透かしを埋め込む前のオリジナルのビデオテープを再生する。再生された映像及び音声は、それぞれ映像出力端子及び音声出力端子から電子透かし埋め込み装置に入力される。また、電子透かし埋め込み装置によって電子透かしが埋め込まれた映像及び音声は、録画側ビデオテープレコーダに入力されて記録される。

【００３４】本装置は、アナログの映像信号を本装置へ取り込む映像入力装置１０１、アナログの音声信号を本装置へ取り込む音声入力装置１０２、入力された映像又は音声をディジタルデータに変換するＡ／Ｄ変換装置１０３、１０４、電子透かし埋め込み装置１０５を有する。

【００３５】上記電子透かし埋め込み装置１０５は、外部からの入力を受ける、又は本装置に入力された映像又は音声データから演算によって、情報を生成する等の方法によって、電子透かしとして埋め込む埋め込み情報を生成し、さらに、不揮発性メモリ１０７に保存されている電子透かしを埋め込む位置を示す座標情報等の鍵データを用い、生成した埋め込み情報を電子透かしとしてコンテンツに埋め込むものである。

【００３６】本装置はさらに、一時的にデータを保存するために用いられる揮発性メモリ１０６、電子透かし埋め込みの埋め込み位置を示す座標データ等から成る鍵データ等が保存される不揮発性メモリ１０７、本装置に搭載されている各装置を制御し、本実施の形態による電子透かし埋め込み方式を実行するコントローラ１０８、本装置で電子透かしの埋め込み処理が行われたディジタルデータをアナログデータに変換するＤ／Ａ変換装置１０９、１１０、本装置によって電子透かしを埋め込まれた映像及び音声を、ビデオテープレコーダ等に対して出力する映像出力装置１１１及び音声出力装置１１２、本装置を構成する各装置間でディジタルデータを交換するのに用いられるデータバス１１３を有している。

【００３７】次に動作について説明する。再生側ビデオテープレコーダで再生され、その映像出力端子から出力されたアナログ画像データは、本電子透かし埋め込み装置の映像入力装置１０１から入力され、Ａ／Ｄ変換装置１０３でディジタルデータに変換されて、揮発性メモリ１０６に保存される。同様に再生側ビデオテープレコーダの音声出力端子から出力されたアナログ音声データは、音声入力装置１０２から入力され、Ａ／Ｄ変換装置１０４によりディジタルデータに変換されて、揮発性メモリ１０６に保存される。

【００３８】電子透かし埋め込み装置１０５では、揮発性メモリ１０６に保存されている映像及び／又は音声データを用いて演算を行う、或いは外部から入力を受ける等の方法で、電子透かしとして埋め込む埋め込みデータを生成する。次に、電子透かし埋め込み装置１０５は、不揮発性メモリ１０７に保存されている鍵データを用いて、上記生成した埋め込みデータを電子透かしとして映像及び／又は音声データに埋め込む。

【００３９】電子透かしが埋め込まれた映像及び／又は音声データは各々Ｄ／Ａ変換装置１０９、１１０によりアナログ化される。アナログ化された映像信号は、映像出力装置１１１により録画側ビデオテープレコーダの映像入力端子に入力され、アナログ化された音声信号は、音声出力装置１１２により録画側ビデオテープレコーダの音声入力端子に入力されて、それぞれ記録される。

【００４０】図２は、図１の電子透かし埋め込み装置により電子透かしが埋め込まれたコンテンツに対して、不正に字幕を入れる、吹き替えを行う等の改竄処理が施された場合に、コンテンツが記録されている記録媒体を再生できないようにした本発明による出力装置の実施の形態を示す。

【００４１】本出力装置は、記録媒体に記憶されている信号を読み取り、音声信号と映像信号に分離して出力するデッキ部２０１、出力制御装置２０７により制御される音声出力装置２０２、同様に出力制御装置２０７により制御される映像出力装置２０３、デッキ部２０１が出力した音声信号及び映像信号をディジタル化して音声データ及び映像データに変換するＡ／Ｄ変換装置２０４、２０５、装置を構成する各装置を制御し、本実施の形態による出力方式を実行するコントローラ２０６を有している。

【００４２】さらに、出力制御装置２０７、一時的にデータや、演算の途中結果などを保存するために用いられる揮発性メモリ２０８、電子透かし埋め込みのための埋め込み位置を示す座標情報等から成る鍵データ等が保存される不揮発性メモリ２０９、本装置を構成する各装置間でディジタルデータを交換するのに用いられるデータバス２１０を有している。

【００４３】次に動作について説明する。デッキ部２０１において記録媒体が再生されると、記録媒体に記録されている信号が読み取られ、音声信号と映像信号に分離される。音声信号は音声出力装置２０２に、映像信号は映像出力装置２０３にそれぞれ入力され一時的に保存される。また、音声信号はＡ／Ｄ変換装置２０４、映像信号はＡ／Ｄ変換装置２０５によりそれぞれディジタルデータ（音声データ及び映像データ）に変換され、揮発性メモリ２０８に一時的に保存される。

【００４４】出力制御装置２０７は、揮発性メモリ２０８より音声データと映像データを取得し、不揮発性メモリ２０９に保存されている鍵データ等を用い、電子透かしとして映像データ、及び／又は音声データに埋め込まれている情報を抽出し、その結果により、音声出力装置２０２、映像出力装置２０３による音声出力、映像出力を決定又は制御する。

【００４５】次に、電子透かし埋め込み装置１０５による具体的な埋め込みデータの生成と電子透かしの埋め込み処理、及び出力制御装置２０７による出力制御処理の各実施の形態について説明する。

【００４６】図３は、電子透かし埋め込み装置１０５で行われる電子透かし埋め込み方式の第１の実施の形態を示すブロック図である。本方式においては、映像をフレームに分割し、各々のフレームにフレーム番号を割り当て、割り当てたフレーム番号を電子透かしとして各フレームに埋め込む。また、音声をブロックに分割し、各々のブロックにブロック番号を割り当て、割り当てたブロック番号を電子透かしとして各ブロックに埋め込む。

【００４７】本方式は、映像データをフレーム毎に分割するフレーム切り出し手段３０１、フレームに先頭から順に番号を付けるフレーム番号生成手段３０２、映像の各フレームにフレーム番号を埋め込む電子透かし埋め込み手段３０３、音声データをブロツクに分割するブロック分割手段３０４、音声ブロックに先頭から順に番号を付けるブロック番号生成手段３０５、音声の各ブロックにブロック番号を埋め込む電子透かし埋め込み手段３０６から構成される。

【００４８】次に動作について説明する。入力された映像データはフレーム切り出し手段３０１により、フレームに分割され、順に出力される。出力された各フレームはフレーム番号生成手段３０２に入力され、順にフレーム番号が生成される。また、各フレームとフレーム番号生成手段３０２により生成されたフレーム番号と不揮発性メモリ１０７に記憶されている電子透かしを埋め込む位置を示す座標情報等からなる鍵データとが電子透かし埋め込み手段３０３に入力され、フレーム番号が各フレームに電子透かしとして埋め込まれ出力される。尚、鍵データが不揮発性メモリから読み込まれずに、外部記憶装置等から入力される場合等の場合もある。

【００４９】音声データについても同様に、ブロック分割手段３０４により、分割されたブロックがブロック番号生成手段３０５に入力され、ブロック番号が生成される。また、各ブロックとブロック番号生成手段３０５によって生成されたブロック番号と電子透かしを埋め込む位置を示す座標情報等からなる鍵データとが電子透かし埋め込み手段３０６に入力され、ブロック番号が各ブロックに電子透かしによって埋め込まれ出力される。

【００５０】ここでの映像出力、音声出力は揮発性メモリ１０６に一時的に保存され同期を取られた後に、Ｄ／Ａ変換装置１０９、１１０によりアナログデータに変換され、映像出力装置１１１、音声出力装置１１２から出力される。

【００５１】図４は、図３の電子透かし埋め込み方式に対応する出力制御方式の第１の実施の形態を示すブロック図であり、図２における出力制御装置２０７に用いられるものである。図４の方式は、図３のフレーム切り出し手段と同じ動作を行うフレーム切り出し手段４０１、映像の各フレームから電子透かしとして埋め込まれているフレーム番号を抽出する電子透かし抽出手段４０２、図３のブロック分割手段と同じ動作を行うブロック分割手段４０３、音声の各ブロックから電子透かしとして埋め込まれているブロック番号を抽出する電子透かし抽出手段４０４、ブロック番号とフレーム番号とを比較し、正しい対応をしているかを調べる比較手段４０５から構成される。

【００５２】次に動作について説明する。入力された映像データはフレーム切り出し手段４０１に入力され、フレーム毎に分割される。各フレームは、電子透かしが埋め込んである位置を示す座標情報等からなる鍵データと共に電子透かし埋め込み手段４０２に入力され、フレーム番号が抽出される。また、入力された音声データは、ブロック分割手段４０３に入力されてブロックに分割され、電子透かし抽出手段４０４において鍵データにより各ブロックからブロック番号が抽出される。

【００５３】電子透かし抽出手段４０２により抽出されたフレーム番号と電子透かし抽出手段４０４により抽出されたブロック番号は比較手段４０５に入力され、正しい対応をしていた場合は、通常出力を許可する信号を発し、この信号により、音声が音声出力装置２０２から、映像が映像出力装置２０３からそれぞれ出力される。

【００５４】図５は、電子透かし埋め込み方式の第２の実施の形態を示すブロック図である。本方式は映像データ、音声データの他に情報の入力を受け、映像と音声に入力された情報を符号化して埋め込むものである。

【００５５】本方式は、映像データをフレーム毎に分割するフレーム切り出し手段５０１、音声データをブロックに分割するブロック分割手段５０２、外部より埋め込み情報を入力する情報入力手段５０３、入力されたデータを埋め込み情報とする符号化手段５０４、映像のフレームに埋め込み情報を電子透かしとして埋め込む電子透かし埋め込み手段５０５、音声のブロックに埋め込み情報を電子透かしとして埋め込む電子透かし埋め込み手段５０６から構成される。

【００５６】入力された映像データはフレーム切り出し手段５０１によって、また音声データはブロック分割手段５０２によって各々フレーム、ブロックに分割される。またキーボード等の情報入力手段５０３によって入力された電子透かしとして埋め込まれる埋め込み情報は、符号化手段５０４によって、誤り訂正符号化等の符号化が施される。符号化された埋め込み情報は、フレーム、鍵データと共に電子透かし埋め込み手段５０５に入力され、電子透かしとして映像のフレームに埋め込まれる。

【００５７】また、埋め込み情報はブロック、鍵データと共に電子透かし埋め込み手段５０６に入力され、電子透かしとして音声のフレームに埋め込まれる。この時、電子透かしは全ての映像フレーム、音声ブロックに埋め込まれる場合の他、一部の映像フレーム、音声ブロックに埋め込まれる場合がある。

【００５８】また、図４の出力制御方式において、比較手段４０５で、所定の映像フレームに埋め込まれている情報と、所定の音声ブロックに埋め込まれている情報とを比較することにより、図５の電子透かし埋め込み方式に対応する出力制御方式を構成できる。この際、埋め込み情報が誤り訂正符号化されている場合は、比較手段４０５は、情報の比較を行う前に誤り訂正符号の復号を行う。

【００５９】図５において、符号化手段５０４が埋め込み情報の誤り訂正符号化を行い、情報ビット又は冗長ビットの一方を映像フレームに、他方を音声ブロックに書き込む電子透かし埋め込み方式も容易に実現可能である。また、図４において、比較手段４０５で、情報ビットを誤り訂正符号化し、求まった冗長ビットと、電子透かしから抽出した冗長ビットとを比較することにより、対応する出力制御方式も容易に構成できる。

【００６０】図５において、符号化手段５０４が所定の埋め込み情報を二つのビット列に分解し、一方を映像フームに、他方を音声ブロックに埋め込む電子透かし埋め込み方式も容易に実現可能である。また、図４の出力制御方式において、比較手段４０５で、抽出された２つの情報を合成し復元した埋め込み方法が上記所定の情報と一致していることを確認することにより、対応する出力制御方式も容易に構成できる。

【００６１】図６は、電子透かし埋め込み方式の第３の実施の形態を示すブロック図である。本方式は、映像フレーム数と同じ数のブロックに音声データを分割し、映像フレームと音声ブロックとを一対一に対応させ、映像フレームに対応する音声ブロックを埋め込むものである。

【００６２】本方式は、映像データをフレームに分割し、１フレームずつ出力するフレーム切り出し手段６０１、映像フレームの１フレームの表示時間と同じ長さに音声データを分割しブロックとするブロック分割手段６０２、映像フレームに音声ブロックを埋め込む電子透かし埋め込み手段６０３から構成される。

【００６３】入力された映像データは、フレーム分割手段６０１によって、フレーム毎に分割され、順に出力される。また、入力された音声データは、ブロック分割手段６０２によって、映像フレームと同じ数に分割され、順に出力される。フレーム分割手段６０１とブロック分割手段６０２の出力を受ける電子透かし埋め込み手段６０３では、電子透かしを埋め込む位置を示す座標情報等

からなる鍵データにより、フレームに、音声ブロックが電子透かしとして埋め込まれて出力される。

【００６４】図７は、図６の電子透かし埋め込み方式に対応する出力制御方式の第２の実施の形態を示すブロック図である。本方式は、映像をフレームに分割するフレーム切り出しし手段７０１、映像フレームに埋め込まれている音声ブロックを抽出する電子透かし抽出手段７０２、Ｄ／Ａ変換手段７０３からなる。Ｄ／Ａ変換手段７０３は、一例として音声出力装置２０２によって処理が実行されるものとする。

【００６５】デッキ部２０１で媒体より読み込まれた映像信号は映像出力装置２０３に入力されるのと同時に、Ａ／Ｄ変換装置２０５によりディジタルデータに変換される。ディジタルデータに変換された映像データは、フレーム切り出し手段７０１によってフレーム毎に分割され、電子透かし抽出手段７０２において、鍵データより、埋め込まれている音声ブロックが抽出される。抽出された音声ブロックは、Ｄ／Ａ変換手段７０３によりアナログデータ化され、音声出力装置２０２によって出力される。

【００６６】図８は電子透かし埋め込み方式の第４の実施の形態を示すブロック図である。本方式では、音声データを映像フレーム数と同じ数のブロックに分割し、映像フレームと音声ブロックとを一対一に対応させる。また、各々の音声ブロックを暗号化し、暗号化音声ブロックを対応する映像フレームに埋め込む。

【００６７】本方式は、図６と同様の動作を行うフレーム切り出し手段６０１、ブロック分割手段６０２、電子透かし埋め込み手段６０３、及び暗号化手段８０１から構成される。ここで用いられる暗号化には、ＤＥＳ等の共通鍵暗号化方式、ＲＳＡ等の公開鍵暗号化方式が用いられる（各暗号の詳細は岡本栄司著「暗号理論入門」共立出版株式会社参照）。

【００６８】入力された音声データは、ブロック分割手段６０２によって、映像フレームと同じ数のブロックに分割された後、入力された暗号鍵により暗号化手段８０１で暗号化されて、電子透かし埋め込み手段６０３において、鍵データにより映像フレームに電子透かしとして埋め込まれて出力される。

【００６９】図９は、図８の電子透かし埋め込み方式に対応する出力制御方式の第３の実施の形態を示すブロック図である。本方式は、図７の出力制御方式と同様の動作を行うフレーム切り出し手段７０１、電子透かし抽出手段７０２、Ｄ／Ａ変換手段７０３、及び図８の暗号化手段８０１に対応する復号手段９０１からなる。

【００７０】入力された映像データは、フレーム切り出し手段７０１によりフレームに分割される。電子透かし抽出処理７０２は、鍵データを用いて各々のフレームより電子透かしとして埋め込まれている音声ブロックを抽出する。抽出された音声ブロックは復号手段９０１により復号された後、Ｄ／Ａ変換手段７０３により音声信号に変換され、音声出力装置２０２によって出力される。

【００７１】図１０は電子透かし埋め込み方式の第５の実施の形態を示すブロック図である。本方式においては、音声をブロックに分割し、ブロック毎に暗号鍵と復号鍵の組を生成し、生成した暗号鍵を用いて音声ブロック再生中に表示されるフレームを暗号化する。また、復号鍵は音声ブロックに電子透かしとして埋め込む。

【００７２】本方式は、映像をフレームに分割するフレーム切り出し手段１００１、暗号鍵と復号鍵の組を生成する鍵生成手段１００２、暗号化手段１００３、音声データをブロックに分割するブロック分割手段１００４、電子透かし埋め込み手段１００５から構成される。ここで用いられる暗号化には、ＤＥＳ等の共通鍵暗号化方式、ＲＳＡ等の公開鍵暗号化方式が用いられる。

【００７３】入力された映像データはフレーム切り出し手段１００１によってフレームに、音声データはブロック分側手段１００４によってブロックに分割される。一方、鍵生成手段１００２では、各々の音声ブロックに対し、暗号鍵と復号鍵の組を生成する。また、暗号化手段１００３では、鍵生成手段１００２で生成された暗号鍵を用い、音声ブロック再生中に表示される映像フレームを暗号化し出力する。また、電子透かし埋め込み手段１００５は、ブロックに分割された音声データへ、鍵生成手段１００２で生成された復号鍵を埋め込み出力する。

【００７４】図１１は、図１０の電子透かし埋め込み方式に対応する出力制御方式の第４の実施の形態を示すブロック図である。本方式は、音声データをブロックに分割するブロック分割手段１１０１、電子透かし抽出手段１１０２、映像データをフレームに分割するフレーム切り出し手段１１０３、フレームに施されている暗号を復号する復号手段１１０４、及び一例としては映像出力装置２０３によって実行されるＤ／Ａ変換手段１１０５から構成される。

【００７５】入力された音声データは、ブロック分割手段１１０１によりブロック毎に分割され、電子透かし抽出手段１１０２に、透かしの埋め込み位置を示す座標情報等からなる鍵データと共に入力される。電子透かし抽出手段１１０２では、電子透かしとして埋め込まれている復号鍵を抽出し、復号手段１１０４に入力する。また、映像データは、フレーム切り出し手段１１０３によって、フレーム毎に分割された後、復号手段１１０４に入力され、復号鍵により復号される。復号されたフレームは、Ｄ／Ａ変換手段１１０５によってアナログ信号に変換され、映像出力装置２０３によって出力される。

【００７６】図１２は電子透かし埋め込み方式の第６の実施の形態を示すブロック図である。本方式においては、音声をブロックに分割し、ブロック毎に暗号鍵と復号鍵の組を生成し、生成した暗号鍵を用いて音声ブロックを嚇号化する。また、復号鍵は音声ブロック再生中に

表示される先頭の映像ブロックに電子透かしとして埋め込む。

【００７７】本方式は、音声をブロックに分割するブロック分割手段１２０１、暗号鍵と復号鍵の組を生成する鍵生成手段１２０２、暗号化手段１２０３、映像データから、対応する音声ブロックの先頭にあたるフレームを抽出するフレーム切り出し手段１２０４、電子透かし埋め込み手段１２０５、及びフレームの順序を整えるための記憶手段１２０６から構成される。

【００７８】入力された音声データはブロック分割手段１２０１によってブロック毎に分割される。また、鍵生成手段１２０２では、音声ブロックと同じ数の暗号鍵と復号鍵の組を生成する。暗号化手段１２０３では、鍵生成手段１２０２で生成された暗号鍵を用い、音声ブロックを暗号化し出力する。また、入力された映像データはフレーム切り出し手段１２０４により音声ブロックの先頭に対応するフレームが抽出され、電子透かし埋め込み手段１２０５により鍵生成手段１２０２で生成された復号鍵が埋め込まれ、さらに記憶手段１２０６に電子透かしが埋め込まれていないフレームと共に入力され、時間的に順序正しく出力される。

【００７９】図１３は、図１２の電子透かし埋め込み方式に対応する出力制御方式の第５の実施の形態を示すブロック図である。本方式は、映像データから音声ブロックの先頭に対応するフレームを抽出するフレーム切り出し手段１３０１、電子透かし抽出手段１３０２、音声データをブロックに分割するブロック分割手段１３０３、音声ブロックに施されている暗号を復号する復号手段１３０４、及び音声出力装置２０２によって実行されるＤ／Ａ変換手段１３０５から構成される。

【００８０】入力された映像データは、フレーム切り出し手段１３０１により音声ブロックの先頭に対応するフレームが抽出される。抽出されたフレームは、電子透かし抽出手段１３０２に、透かしの埋め込み位置を示す座標情報等からなる鍵データと共に入力される。電子透かし抽出手段１３０２では、電子透かしとしてフレームに埋め込まれている復号鍵を抽出し復号手段１３０４に入力する。

【００８１】また、入力された音声データは、ブロック分割手段１３０３により音声ブロックに分割され、復号手段１３０４に入力される。音声ブロックは、復号手段１３０４で、復号鍵により復号され、Ｄ／Ａ変換手段１３０５によりアナログ信号に変換されて、音声出力装置２０２によって出力される。

【００８２】図１４は電子透かし埋め込み方式の第７の実施の形態を示すブロック図である。入力された映像データをフレームに分けるフレーム切り出し手段１４０１、音声データを一定長のブロックに分割するブロック分割手段１４０２、映像データの指定フレームのハッシュ値を求めるハッシュ計算手段１４０３、音声ブロックに映像フレームのハッシュ値を埋め込む電子透かし埋め込み手段１４０４、電子透かし埋め込み済みの音声ブロックのハッシュ値を求めるハッシュ計算手段１４０５、映像フレームのあるフレームに音声ブロックのハッシュ値を埋め込む電子透かし埋め込み手段１４０６、記憶手段１４０７からなる。

【００８３】本方式で用いられているハッシュ値について説明する。ハッシュ値ｈとは、ハッシュ関数ｆ：ｘ→ｈにより求められる長い入力列ｘの圧縮値である短い出力ｈである。また、一方向性関数であり、ｆ（ｘ’）＝ｆ（ｘ）を満たす、異なる入力ｘ，ｘ’を求めるのは難しいという性質を持つ。ハッシュ関数の代表的なものとして、ＭＤ５（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ５）、ＳＨＡ（ＳｅｃｕｒｅＨａｓｈＡｌｇｏｒｉｔｌｈｍ）等がある。ハッシュ関数の詳細については、岡本栄司著「暗号理論入門」（共立出版株式会社）に詳しい。

【００８４】入力された映像データは記憶手段１４０７に保存される他、フレーム切り出し手段１４０１によって、ハッシュ値を求められるハッシュフレーム及び音声ブロックのハッシュ値が埋め込まれる埋め込みフレームが抽出される。また、音声データはブロック分割手段１４０２によって、所定長のブロックに分割される。ここで、音声データの１ブロックに対応する時間の中に、ハッシュフレーム、埋め込みフレームが１つずつ存在する様にフレーム抽出、ブロック分割が行われる。

【００８５】ハッシュ計算手段１４０３は、フレーム切り出し手段１４０１によって求められたハッシュフレームよりハッシュ値を計算する。電子透かし埋め込み手段１４０４は、電子透かしを埋め込む位置を示す座標情報等からなる鍵データを用いて、ハッシュ値を音声ブロックの中に埋め込む。電子透かしが埋め込まれた音声ブロックは、音声出力として出力される他、ハッシュ計算手段１４０５に入力されハッシュ値が求められる。求められたハッシュ値は電子透かし埋め込み手段１４０６に入力され、鍵データによって埋め込みフレームの中に電子透かしとして埋め込まれる。

【００８６】電子透かしが埋め込まれた埋め込みフレームは記憶手段１４０７に記憶されているオリジナルの映像データの対応するフレームと置き換えられて保存される。記憶手段１４０７に埋め込み対象フレームが保存された後、記憶手段１４０７に保存されている映像データが映像出力として出力される。

【００８７】図１５は、図１４の電子透かし埋め込み方式に対応する出力制御方式の第６の実施の形態を示すブロック図である。この出力制御方式は、音声データを所定の長さのブロックに分割するブロック分割手段１５０１、映像データからハッシュフレームと埋め込みフレームを抽出するフレーム切り出し手段１５０２、音声ブロックのハッシュ値を計算するハッシュ計算手段１５０３、映像データのハッシュフレームのハッシュ値を計算

するハッシュ計算手段１５０４、音声ブロックに埋め込まれているハッシュ値を抽出する電子透かし抽出手段１５０５、埋め込みフレームに埋め込まれている音声ブロックのハッシュ値を抽出する電子透かし抽出手段１５０６、音声ブロックから計算したハッシュ値と埋め込みフレームから抽出したハッシュ値とを比較する比較手段１５０７、ハッシュフレームから計算したハッシュ値と音声ブロックから抽出したハッシュ値とを比較する比較手段１５０８から構成される。

【００８８】入力された音声データは、ブロック分割手段１５０１によって、所定の長さのブロックに分割される。分割されたブロックは１ブロック毎にハッシュ計算手段１５０３に入力され、ハッシュ値が計算される。同時に電子透かし抽出手段１５０５にも入力され、電子透かしとして埋め込まれている映像データのハッシュフレームのハッシュ値が抽出される。

【００８９】また、入力された映像データはフレーム切り出し手段１５０２に入力され、ハッシュフレームと埋め込みフレームが抽出される。ハッシュフレームはハッシュ計算手段１５０４に入力され、ハッシュ値が計算される。また、埋め込みフレームは電子透かし抽出手段１５０６に入力され、埋め込まれているハッシュ値が抽出される。ハッシュ計算手段１５０３により計算された音声ブロックのハッシュ値と、電子透かし抽出手段１５０６により埋め込みフレームより抽出されたハッシュ値は比較手段１５０７に入力され比較される。

【００９０】各ハッシュ値が一致していた場合、即ち、音声データがオリジナルの音声データと一致していると判断される場合は、音声出力装置２０２が音声を出力するよう制御信号を発する。各ハッシュ値が一致していなかった場合には、音声出力装置２０２は何も出力せずに、保存していた音声ブロックを捨てるように制御信号を発する。

【００９１】また、ハッシュ計算手段１５０４によりハッシュフレームから計算されたハッシュ値と、電子透かし抽出手段１５０５により音声ブロックから抽出されたハッシュ値は比較手段１５０８に入力され比較される。各ハッシュ値が一致していた場合、即ち、映像データがオリジナルの映像データと一致していると判断される場合は、映像出力装置２０３が映像を出力するよう制御信号を発し、各のハッシュ値が一致していなかった場合は、映像出力装置２０３は何も出力せずに、保存していたデータを捨てるように制御信号を発する。

【００９２】図１６は電子透かし埋め込み方式の第８の実施の形態を示すブロック図である。本方式は、図１４と同様の動作を行うフレーム切り出し手段１４０１、ブロック分割手段１４０２、ハッシュ計算手段１４０３、電子透かし埋め込み手段１４０４、ハッシュ計算手段１４０５、電子透かし埋め込み手段１４０６、記憶手段１４０７、及びハッシュ計算手段１４０３．１４０５によって求めたハッシュ値を暗号化する暗号化手段１６０１、１６０２から構成される。

【００９３】ハッシュ計算手段１４０３によって生成されたハッシュフレームのハッシュ値は暗号化手段１６０１で入力された暗号鍵により暗号化された後、電子透かし埋め込み手段１４０４によって、音声ブロックに埋め込まれる。また、ハッシュ計算手段１４０５によって生成された音声ブロックのハッシュ値は暗号化手段１６０２で入力された暗号鍵により暗号化された後、電子透かし埋め込み手段１４０６によって埋め込みフレームに埋め込まれる。

【００９４】暗号化手段を持ちいたことにより、映像のハッシュフレームを改竄した場合、例えハッシュ関数が判っても暗号鍵が判らなければ音声ブロックに埋め込むデータを求めることができない。従って、より高度なセキュリティを確保できる。ここで用いられる暗号化には、ＤＥＳ等の共通鍵暗号化方式、ＲＳＡ等の公開鍵暗号化方式が用いられる。ここで、ＲＳＡ等の公開鍵暗号方式を用い、その秘密鍵で暗号化を行った場合、求められる値は、ディジタル署名となる。

【００９５】図１７は、図１６の電子透かし埋め込み方式に対応する出力制御方式の第７の実施の形態を示すブロック図である。本方式は、図１５と同様の動作を行う、ブロック分割手段１５０１、フレーム切り出し手段１５０２、ハッシュ計算手段１５０３、１５０４、電子透かし抽出手段１５０５、１５０６、比較手段１５０７、１５０８、及び図１６の暗号化手段１６０１、１６０２に対応する復号手段１７０１、１７０２から成る。

【００９６】電子透かし抽出手段１５０５により音声ブロックから抽出された暗号化されたハッシュフレームは、復号手段１７０１と入力された復号鍵によって復号される。また、電子透かし抽出手段１５０６により埋め込みフレームから抽出された、暗号化された音声フレームは復号手段１７０２と入力された復号鍵によって復号される。以下の動作は図１５の出力制御方式と同様である。

【００９７】ここで、一例として、電子透かし抽出手段１５０５．１５０６によりディジタル署名が抽出された場合、復号手段１７０１、１７０２では、署名生成に用いられた秘密鍵に対応する公開鍵で復号を行う。

【００９８】図１８は、図１６の電子透かし埋め込み方式に対応する出力制御方式の第８の実施の形態を示すブロック図である。本方式は、図１５と同様の動作を行うブロック分割手段１５０１、フレーム切り出し手段１５０２、ハッシュ計算手段１５０３、１５０４、電子透かし抽出手段１５０５、１５０６、比較手段１５０７、１５０８、及び図１６と同様の動作を行う暗号化手段１６０１、１６０２から構成される。

【００９９】ハッシュ計算手段１５０４により計算されたハッシュ値は、暗号化手段１６０１に入力され、図１

６の電子透かし埋め込み手段で電子透かし埋め込み時に用いた暗号鍵と同一の暗号鍵で暗号化され、比較手段１５０８に入力される。同様にハッシュ計算手段１５０３で求められたハッシュ値は、暗号化手段１６０２で暗号化され、比較手段１５０７に入力される。他の動作は図１５の出力制御方式と同様である。

【０１００】ここでは一例として、アナログオーディオビデオコンテンツを扱う電子透かし埋め込み装置及び出力装置を挙げたが、他のアナログコンテンツ、及びディジタルオーディオビデオコンテンツ等ディジタルコンテンツ等を扱うディジタルビデオ機器等、その他のコンテンツに対し透かしを埋め込む電子透かし埋め込み装置、制御を行う出力装置等も本発明の範疇に含む。

【０１０１】また、図１に示した電子透かし埋め込み装置より、Ａ／Ｄ変換装置１０３、１０４及びＤ／Ａ変換装置１０９、１１０を削除することにより、ディジタルコンテンツを扱うディジタル機器に使用可能である電子透かし埋め込み装置が構成される。

【０１０２】また、図２に示した出力装置より、Ａ／Ｄ変換装置２０４，２０５を削除することにより、ディジタルコンテンツを扱うディジタル出力機器が構成される。また、ＭＰＥＧ－４画像等、複数のオブジェクトを含むコンテンツにおいて、各々のオブジェクトに対し透かしを埋め込み、制御を行う方法及び装置等も本発明の範薦に含む。

【０１０３】また、図１における埋め込み装置１０５において、フレーム切り出し手段及びフロック分割手段の代わりに、ＭＰＥＧ－４画像よりオブジェクトを抽出するオブジェクト抽出処理を設けることにより、ＭＰＥＧ－４画像に対する電子透かし埋め込み装置が構成される。また、図２に示した出力装置における出力制御装置がフレーム切り出し手段及びブロック分割手段の代わりにオブジェクトを抽出する処理を行うことにより、ＭＰＥＧ－４画像に埋め込まれた電子透かしにより出力を制御する出力装置が構成される。

【０１０４】また、上記の電子透かし埋め込み方式を組み合わせることにより、よりセキュリティの高い電子透かし埋め込み方式が構成される。さらに、上記の出力制御方式を組み合わせ用いることにより、上記電子透かし埋め込み方式をこの組み合わせにより生成した電子透かし埋め込み方式によって電子透かしを埋め込んだコンテンツから、電子透かしを抽出し、出力を制御する出力制御方式が容易に構成される。

【０１０５】次に本発明の他の実施の形態としての記憶媒体について説明する。本発明はハードウェアで構成することもできるが、ＣＰＵとメモリとで構成されるコンピュータシステムで構成することもできる。コンピュータシステムで構成する場合、上記メモリは本発明による記憶媒体を構成する。即ち、前述した各実施の形態で説明した動作を実行するためのソフトウェアのプログラムコードを記憶した記憶媒体をシステムや装置で用い、そのシステムや装置のＣＰＵが上記記憶媒体に格納されたプログラムコードを読み出し、実行することにより、本発明の目的を達成することができる。

【０１０６】また、この記憶媒体としては、ＲＯＭ、ＲＡＭ等の半導体メモリ、光ディスク、光磁気ディスク、磁気媒体等を用いてよく、これらをＣＤ－ＲＯＭ、フロッピィディスク、磁気媒体、磁気カード、不揮発性メモリカード等に構成して用いてよい。

【０１０７】従って、この記憶媒体を各図に示したシステムや装置以外の他のシステムや装置で用い、そのシステムあるいはコンピュータがこの記憶媒体に格納されたプログラムコードを読み出し、実行することによっても、上記各実施の形態と同等の機能を実現できると共に、同等の効果を得ることができ、本発明の目的を達成することができる。

【０１０８】また、コンピュータ上で稼働しているＯＳ等が処理の一部又は全部を行う場合、あるいは記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された拡張機能ボードやコンピュータに接続された拡張機能ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づいて、上記拡張機能ボードや拡張機能ユニットに備わるＣＰＵ等が処理の一部又は全部を行う場合にも、上記各実施の形態と同等の機能を実現できると共に、同等の効果を得ることができ、本発明の目的を達成することができる。

【０１０９】

【発明の効果】以上説明したように、本発明によれば、複数の情報系列としての映像及び音声を相互に関連を持たせた電子透かし埋め込みを実現することができると共に、映像及び音声を組み合わせた電子透かし埋め込みを実現することができ、これにより、映像と音声の両方を有するコンテンツの総合的な著作権保護方式が可能となった。

【０１１０】また、本発明によれば、電子透かしが埋め込まれたコンテンツに改竄等の不正が行われた場合は、それを検知してコンテンツの出力を禁止する等の制御を行うことができる。

【図面の簡単な説明】

【図１】本発明による電子透かし埋め込み装置の実施の形態を示すブロック図である。

【図２】本発明による出力制御装置を用いた出力装置の実施の形態を示すブロック図である。

【図３】本発明による電子透かし埋め込み装置で行われる電子透かし埋め込み方式の第１の実施の形態を示すブロック図である。

【図４】本発明による出力制御装置で行われる出力制御方式の第１の実施の形態を示すブロック図である。

【図５】電子透かし埋め込み方式の第２の実施の形態を示すブロック図である。

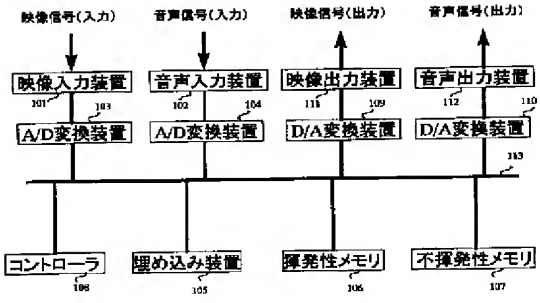
２３

【図６】電子透かし埋め込み方式の第３の実施の形態を示すブロック図である。
【図７】出力制御方式の第２の実施の形態を示すブロック図である。
【図８】電子透かし埋め込み方式の第４の実施の形態を示すブロック図である。
【図９】出力制御方式の第３の実施の形態を示すブロック図である。
【図１０】電子透かし埋め込み方式の第５の実施の形態を示すブロック図である。
【図１１】出力制御方式の第４の実施の形態を示すブロック図である。
【図１２】電子透かし埋め込み方式の第６の実施の形態を示すブロック図である。
【図１３】出力制御方式の第５の実施の形態を示すブロック図である。
【図１４】電子透かし埋め込み方式の第７の実施の形態を示すブロック図である。
【図１５】出力制御方式の第６の実施の形態を示すブロック図である。
【図１６】電子透かし埋め込み方式の第８の実施の形態を示すブロック図である。
【図１７】出力制御方式の第７の実施の形態を示すブロック図である。
【図１８】出力制御方式の第８の実施の形態を示すブロック図である。
【符号の説明】

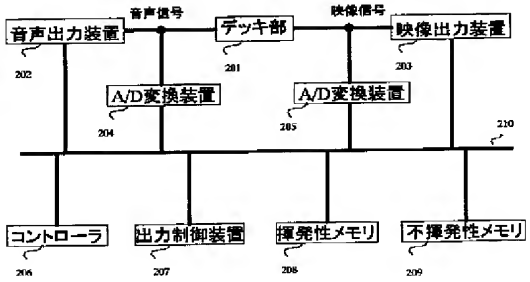
２４

１０５　埋め込み装置
１０８、２０６　コントローラ
２０７　出力制御装置
３０１、４０１、５０１、６０１、７０１、１００１、１１０３、１２０４、１３０１、１４０１、１５０２　フレーム切り出し手段
３０２　フレーム番号生成手段
３０３、３０６、５０５、５０６、６０３、１００５、１２０５、１３０２、１４０４、１４０６　電子透かし埋め込み手段
３０４、４０３、５０２、６０２、１００４、１１０１、１２０１、１３０３、１５０１　ブロック分割手段
３０５　ブロック番号生成手段
４０２、４０４、７０２、１１０２、１３０２、１５０５、１５０６　電子透かし抽出手段
４０５、１５０７、１５０８　比較手段
５０３　情報入力手段
５０４　符号化手段
８０１、１００３、１２０３、１６０１、１６０２　暗号化手段
９０１、１１０４、１３０４、１７０１、１７０２　復号手段
１００２、１２０２　鍵生成手段
１２０６、１４０７　記憶手段
１４０３、１４０５、１５０３、１５０４　ハッシュ計算手段

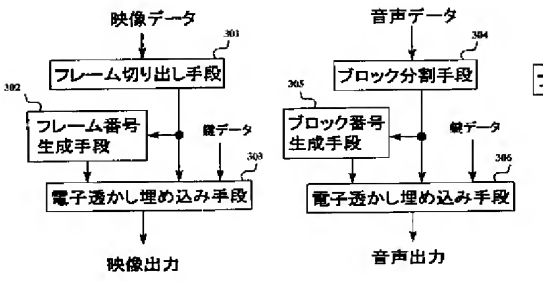
【図１】



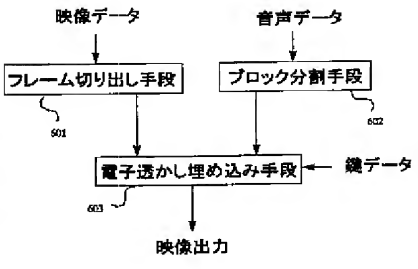
【図２】



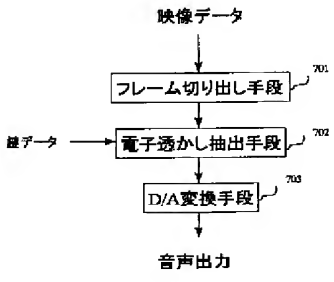
【図３】



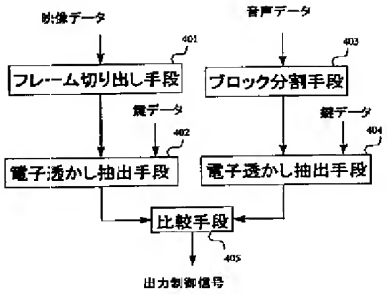
【図６】



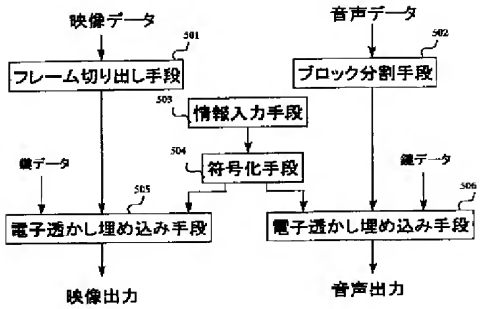
【図７】



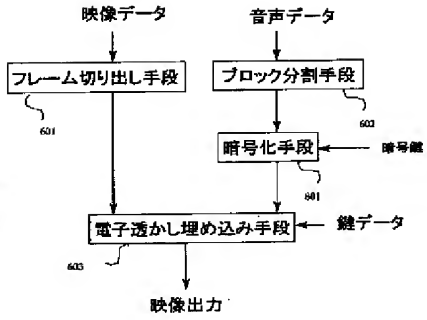
【図４】



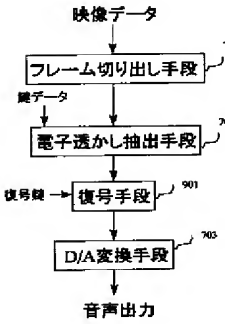
【図５】



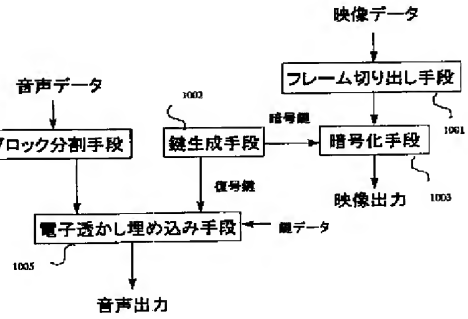
【図８】



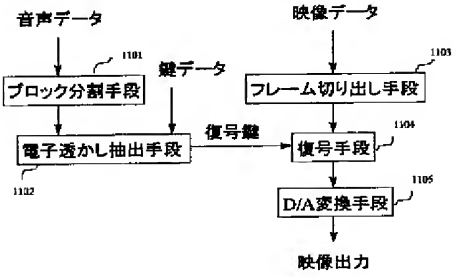
【図９】



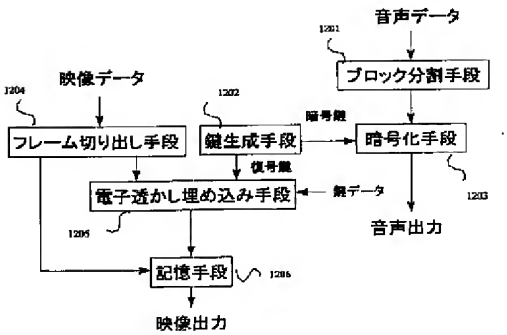
【図１０】



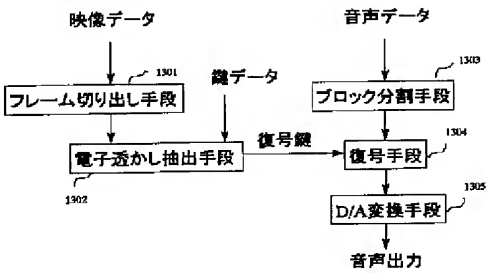
【図１１】



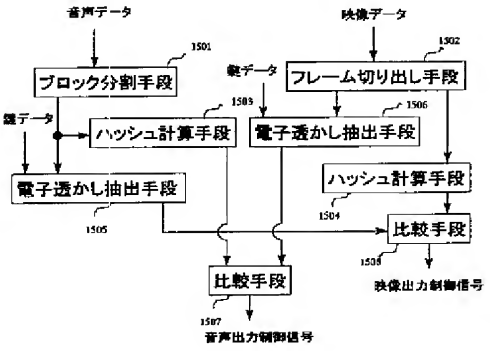
【図１２】



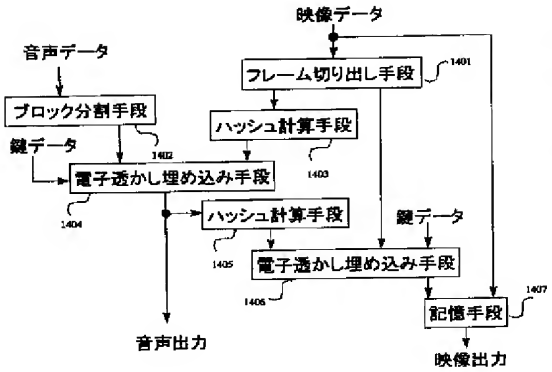
【図１３】



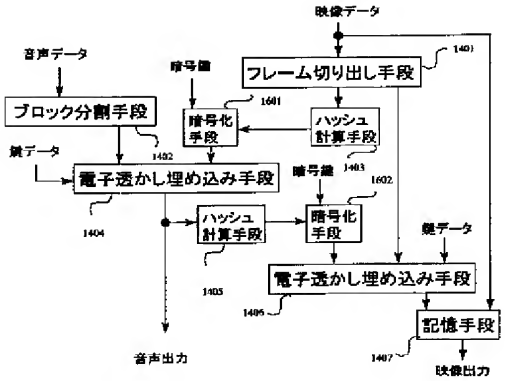
【図１５】



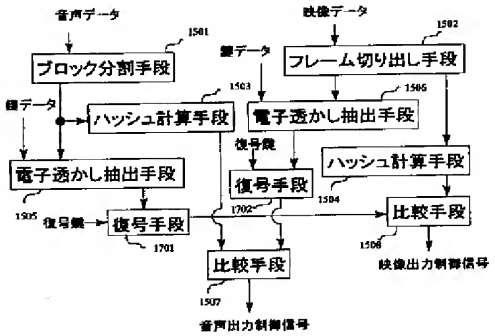
【図１４】



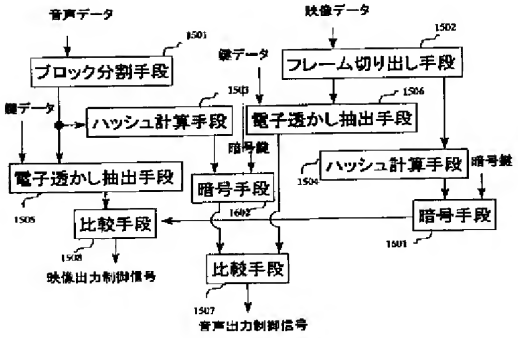
【図１６】



【図１７】



【図１８】



フロントページの続き

Ｆターム(参考)　5C063 AB03 AB07 AC01 AC05 AC10
CA05 CA09 CA20 CA23 CA40
5C076 AA14 AA40 BA06
5J064 AA00 CA02 CC07
5J104 AA14 EA17 EA20 PA05 PA14
9A001 EE03 EE04 HH15 HH27